

UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA,

v.

ROMAN STORM, ET AL.,

Defendants.

Case No. 23 Cr. 430 (KPF)

Final Pretrial Conference: July 8, 2025

**DEFENDANT ROMAN STORM'S  
COMBINED MOTIONS IN LIMINE (1-10)**

Brian E. Klein  
Keri Curtis Axel  
Becky S. James  
Kevin M. Casey  
Viviana Andazola Marquez  
Waymaker LLP  
515 S. Flower Street, Suite 3500  
Los Angeles, California 90071  
(424) 652-7800

David E. Patton  
Nicholas D. Pavlis  
Hecker Fink LLP  
350 Fifth Ave, 63rd Floor  
New York, New York 10118  
(212) 763-0883

*Attorneys for Roman Storm*

**TABLE OF CONTENTS**

	<b><u>Page</u></b>
I. PRELIMINARY STATEMENT .....	1
II. LEGAL STANDARD.....	1
III. ARGUMENT.....	2
A. MIL No. 1: This Court Should Preclude the Government from Making References to the Lazarus Group.....	2
1. Any Allegations Claiming that the Lazarus Group Conducted Criminal Hacks and Used Tornado Cash Should Be Excluded for Lack of Evidence .....	4
2. In Any Event, the Identity of the Lazarus Group Is Not Relevant .....	7
3. Any Possible Probative Value of the Identity of the Lazarus Group Is Far Outweighed by Its Prejudicial Effect.....	9
B. MIL No. 2: This Court Should Preclude the Government from Introducing Victim Testimony or Referencing Victim Impacts Regarding the Lazarus Group’s Hacking.....	11
1. Victim Impacts Are Irrelevant in This Case .....	11
2. The Prejudicial Effect of Victim Testimony or References Would Substantially Outweigh Any Probative Value .....	12
C. MIL No. 3: This Court Should Preclude the Government from Offering Evidence or Argument Related to North Korea’s Military, Including Its Weapons and Nuclear Missile Programs .....	13
D. MIL No. 4: This Court Should Preclude the Government from Introducing Evidence or Argument Regarding So-Called Tornado Cash “Marketing Materials” that Allegedly Depict a Washing Machine .....	14
E. MIL No. 5: This Court Should Preclude the Government from Introducing Any Evidence of Mr. Storm’s Alleged TORN Sales.....	16
F. MIL No. 6: This Court Should Preclude the Government from Characterizing Mr. Storm’s Alleged Sales of TORN Using Language that Reflects a Legal Conclusion or Is Inflammatory, Confusing, or Unduly Prejudicial, Including by Referencing His Russian Background.....	21
G. MIL No. 7: This Court Should Preclude the Government from Introducing Evidence or Argument Referencing OFAC’s Imposition of Sanctions on Tornado Cash Without Mentioning That The Sanctions Were Held to Be Unlawful .....	24
H. MIL No. 8: This Court Should Preclude the Government From Arguing That Anonymous Blockchain Activity or Crypto-Mixing Is Illicit .....	27

I.	MIL No. 9: This Court Should Preclude the Government and Its Witnesses from Referring to Tornado Cash as a “Service” and Its Users as “Customers” .....	29
1.	This Court Should Preclude the Government’s Witnesses From Using the Terms “Service” and “Customer” Because the Terms Imply Legal Conclusions .....	30
2.	The Terms “Service” and “Customer” Are Not Probative and Are Unduly Prejudicial .....	34
J.	MIL No. 10: This Court Should Preclude the Government and Its Witnesses From Offering Improper Summary Charts or Summary Testimony .....	35
IV.	CONCLUSION.....	40

**TABLE OF AUTHORITIES****Page****CASES**

<i>Aristocrat Leisure Ltd. v. Deutsche Bank Trust Co. Americas.</i> , 2009 WL 3111766 (S.D.N.Y. Sept. 28, 2009).....	22
<i>Arlio v. Lively</i> , 474 F.3d 46 (2d Cir. 2007).....	2
<i>Dep't of Treasury, et al.</i> , Case No. 23-13698, ECF Nos. 54 (11th Cir. Apr. 21, 2025).....	25
<i>Doe v. Lima</i> , 2020 WL 728813 (S.D.N.Y., Feb. 13, 2020).....	13
<i>FAA v. Landy</i> , 705 F.2d 624 (2d Cir. 1983).....	31
<i>Highland Cap. Mgmt., L.P. v. Schneider</i> , 551 F. Supp. 2d 173 (S.D.N.Y. 2008).....	34
<i>In re Term Commodities Cotton Futures Litig.</i> , 2020 WL 5849142 (S.D.N.Y. Sept. 30, 2020).....	31
<i>MF Global Holdings, Ltd. v. PricewaterhouseCoopers LLP</i> , 232 F. Supp.3d 558 (S.D.N.Y. 2017).....	22, 23
<i>Old Chief v. United States</i> , 519 U.S. 172 (1997).....	2, 9, 23
<i>Peat, Inc. v. Vanguard Research, Inc.</i> , 378 F.3d 1154 (11th Cir. 2004) .....	38
<i>United States v. Al-Moayad</i> , 545 F.3d 139 (2d Cir. 2008).....	10
<i>United States v. Araujo</i> , 539 F.2d 287 (2d Cir. 1976).....	11
<i>United States v. Banki</i> , 685 F.3d 99 (2d Cir. 2012).....	22
<i>United States v. Bermudez</i> , 529 F.3d 158 (2d Cir.2008).....	12
<i>United States v. Birney</i> , 686 F.2d 102 (2d Cir. 1982).....	2

<i>United States v. Bray</i> , 139 F.3d 1104 (6th Cir. 1998) .....	38, 39
<i>United States v. Duncan</i> , 42 F.3d 97 (2d Cir. 1994) .....	33
<i>United States v. Elfgeeh</i> , 515 F.3d 100 (2d Cir. 2008).....	10
<i>United States v. Figueroa</i> , 618 F.2d 934 (2d Cir. 1980).....	2
<i>United States v. Fullwood</i> , 342 F.3d 409 (5th Cir. 2003) .....	38
<i>United States v. Gleason</i> , 616 F.2d 2 (2d Cir. 1979) .....	24
<i>United States v. Gotti</i> , 459 F.3d 296 (2d Cir. 2006).....	7
<i>United States v. Guo</i> , 2024 WL 2262706 (S.D.N.Y. May 17, 2024) .....	29
<i>United States v. Hendricks</i> , 921 F.3d 320 (2d Cir. 2019).....	12
<i>United States v. Jacques Dessange, Inc.</i> , 2000 WL 294849 (S.D.N.Y. Mar. 21, 2000) .....	33
<i>United States v. Johnson</i> , 54 F.3d 1150 (4th Cir. 1995) .....	38
<i>United States v. Klein</i> , 2017 WL 1316999 (E.D.N.Y. Feb. 10, 2017).....	27
<i>United States v. Lemire</i> , 720 F.2d 1327 (D.C. Cir. 1983).....	38
<i>United States v. Livoti</i> , 196 F.3d 322 (2d Cir. 1999).....	2
<i>United States v. Malka</i> , 602 F. Supp. 3d 510 (S.D.N.Y. 2022).....	12
<i>United States v. Maxwell</i> , 20 CR 330 (AJN), (Dec. 9, 2021) .....	37
<i>United States v. Murgio</i> , 209 F. Supp. 3d 698 (S.D.N.Y. 2016).....	8

<i>United States v. Neil Phillips</i> , ECF No. 90 at 2, (S.D.N.Y. Oct. 20, 2023) .....	36, 39, 40
<i>United States v. Paccione</i> , 949 F.2d 1183 (2d Cir. 1991).....	12
<i>United States v. Patel</i> , 2023 WL 2643815 (D. Conn. Mar. 27, 2023) .....	34
<i>United States v. Ray</i> , No. 20 Cr. 110 (LJL), 2022 WL 558146 (S.D.N.Y. Feb. 24, 2022).....	31
<i>United States v. Scop</i> , 846 F.2d 135 (2d Cir. 1988).....	31
<i>United States v. Smothers</i> , 652 F. Supp. 3d 271 (E.D.N.Y. 2023) .....	22
<i>United States v. Sterlingov</i> , 2023 WL 2387759 (D.D.C. Mar. 6, 2023).....	28
<i>United States v. Velastegui</i> , 199 F.3d 590 (2d Cir. 1999).....	17, 32
<i>United States v. Wagner</i> , 2022 WL 19179 (S.D.N.Y. Jan. 3, 2022) .....	31
<i>Van Loon v. Dep't of Treasury</i> , No. 23-50669, 2024 WL 1771719 (5th Cir. Apr. 15, 2024) .....	passim
<i>Van Loon v. Dept of the Treasury</i> , No. 1:23-cv-312-RP, ECF No. 107 (W.D. Tex., Mar. 21, 2025) .....	25, 26, 27
<i>Walker v. Time Life Films, Inc.</i> , 784 F.2d 44 (2d Cir. 1986).....	35

## **STATUTES**

18 U.S.C. § 1956(a)(1).....	16
18 U.S.C. § 1960.....	8, 22, 32

## **FEDERAL STATUTES**

Federal Evidence § 403.04[1][b] .....	34
---------------------------------------	----

**RULES**

Fed. R. Evid. 1006 .....	35, 36, 38
Fed. R. Evid. 105 .....	39
Fed. R. Evid. 107 .....	37, 39, 40
Fed. R. Evid. 401 .....	passim
Fed. R. Evid. 402 .....	passim
Fed. R. Evid. 403 .....	passim
Fed. R. Evid. 611(a).....	35, 37

**OTHER SOURCES**

The Law and Politics of Cyberattack Attribution, 67 UCLA L. REV. 520, 567 (2020).....	5
--	---

## **I. PRELIMINARY STATEMENT**

Defendant Roman Storm respectfully submits this memorandum in support of the following motions *in limine* to preclude the government, and its witnesses where applicable, from:

- A. MIL No. 1: Making references to the Lazarus Group;
- B. MIL No. 2: Introducing victim testimony or referencing victim impacts regarding the Lazarus Group's hacking;
- C. MIL No. 3: Introducing evidence or argument related to North Korea's military, including its weapons and nuclear missile programs;
- D. MIL No. 4: Offering any evidence or argument regarding so-called Tornado Cash "marketing materials" that allegedly depict a washing machine;
- E. MIL No. 5: Introducing any evidence of Mr. Storm's alleged TORN sales;
- F. MIL No. 6: Characterizing Mr. Storm's alleged sales of TORN using language that reflects a legal conclusion or is inflammatory, confusing, or unduly prejudicial, including by referencing his Russian background;
- G. MIL No. 7: Introducing evidence or argument referencing OFAC's imposition of sanctions on Tornado Cash without mentioning that the sanctions were held to be unlawful;
- H. MIL No. 8: Arguing that anonymous blockchain activity or cryptocurrency mixing is illicit;
- I. MIL No. 9: Referring to Tornado Cash as a "service" and its users as "customers"; and
- J. MIL No. 10: Offering improper summary charts or summary testimony.

For the reasons discussed below, this Court should not permit the government to offer such evidence, argument, and witness testimony at Mr. Storm's upcoming trial pursuant to various Federal Rules of Evidence.

## **II. LEGAL STANDARD**

Evidence is relevant if it "has any tendency to make a fact more or less probable than it would be without the evidence; and the fact is of consequence in determining the action." Fed.



R. Evid. 401. If a piece of evidence tends to establish a fact “that is of consequence to the determination of the action, then it is relevant. If it does not tend to prove a material fact, it is irrelevant.” *Arlio v. Lively*, 474 F.3d 46, 52 (2d Cir. 2007). “Irrelevant evidence is not admissible.” Fed. R. Evid. 402.

Even if evidence is both relevant and otherwise admissible, courts may nonetheless exclude such evidence if “its probative value is substantially outweighed by a danger of...unfair prejudice, confusing the issues, misleading the jury, undue delay, wasting time, or needlessly presenting cumulative evidence.” Fed. R. Evid. 403. The term “unfair prejudice,” with respect to a criminal defendant, “speaks to the capacity of some concededly relevant evidence to lure the factfinder into declaring guilt on a ground different from proof specific to the offense charged.” *Old Chief v. United States*, 519 U.S. 172, 180 (1997). As such, in determining whether evidence is unfairly prejudicial, a court may consider the context of the alleged crime and will exclude evidence when it is “more inflammatory than the charged crime.” *United States v. Livoti*, 196 F.3d 322, 326 (2d Cir. 1999); *see United States v. Birney*, 686 F.2d 102, 106 (2d Cir. 1982) (citing Fed. R. Evid. 403, Advisory Committee Note) (“[U]nfair prejudice means an undue tendency to suggest decision on an improper basis, commonly, though not necessarily, an emotional one.”). In other words, unfair prejudice may result if evidence tends “to prove some adverse fact not properly in issue or unfairly to excite emotions against the defendant.” *United States v. Figueroa*, 618 F.2d 934, 943 (2d Cir. 1980).

### III. ARGUMENT

#### A. **MIL No. 1: This Court Should Preclude the Government from Making References to the Lazarus Group**

Mr. Storm is charged with three counts of conspiracy: (1) money laundering; (2) operating an unlicensed money transmitting business; and (3) violating the International

Emergency Economic Powers Act (“IEEPA”). (*See* Dkt. 1 (“Ind.”).)<sup>1</sup> The heart of the government’s allegations is that a third-party, the so-called “Lazarus Group,” purportedly utilized the Tornado Cash protocol to launder criminal proceeds from a supposed hacking operation and to evade sanctions against North Korea. (*See, e.g., id.* at ¶¶ 1, 55, 60-61, 65-68, 85-88.) Mr. Storm is not charged with hacking, nor is he alleged to have conspired with or have any ties to the Lazarus Group. In fact, the government has conceded that it does not allege that Mr. Storm conspired with any Tornado Cash user, including the Lazarus Group, to violate the federal money laundering statute. (*See* Gov’t Opp. to Pretrial Mots., Dkt. 53 at 40.)

Nevertheless, given the lengthy allegations in the Indictment discussing the Lazarus Group, the defense anticipates that the government will attempt to contend that the group conducted criminal hacks, including the alleged cyber-attack known as the “Ronin hack,” and that the group is connected to the North Korean government. (*See, e.g., Ind.* ¶¶ 55-61, 66-67, 73.) There are two major problems with these contentions: (1) the government has produced no evidence supporting the contention that the Ronin hack was conducted by the Lazarus Group (which is itself a catch-all term describing cybercriminals sponsored by North Korea but affiliating in different subgroups for different purposes); and (2) in any event, the identity of the Lazarus Group, and particularly its association with North Korea, is not relevant to the charges here and is substantially more prejudicial than probative. Accordingly, Mr. Storm moves for an order precluding references by the government at trial to the Lazarus Group, including any argument or evidence regarding the nationality or nature of the group, due to the irrelevance and unfair prejudice of any such references.

---

<sup>1</sup> All references in this motion are to the original speaking Indictment, Dkt. 1, unless otherwise indicated.

**1. Any Allegations Claiming that the Lazarus Group Conducted Criminal Hacks and Used Tornado Cash Should Be Excluded for Lack of Evidence**

The government has produced no evidence, including from a testifying expert or even a qualified government authority,<sup>2</sup> that proves that the Lazarus Group (whatever it actually is) conducted any hack. While the Indictment contains numerous inflammatory allegations concerning the Lazarus Group, as discussed further below, the “evidence” does not support these statements. Indeed, the government’s proposed testifying witnesses themselves are not experts in North Korean money laundering and offer no opinions that the Lazarus Group conducted the hacks.<sup>3</sup> Without reliable evidence to attribute the Ronin Hack to the Lazarus Group, evidence regarding the Lazarus Group is irrelevant as the group bears no demonstrated connection to this case. *See* Fed. R. Evid. 401, 402.

In the Indictment, the only support offered for the Lazarus Group’s purported involvement in the Ronin hack is the reference to an FBI-issued three-sentence press release with no supporting evidence. (*See* Ind. ¶ 60 (citing Apr. 14 2022 FBI Press Release).)<sup>4</sup> That press release is inadmissible hearsay under Federal Rules of Evidence 801 and 802, and the government has offered no other evidence that would attribute any hack to the Lazarus Group.

---

<sup>2</sup> True and correct copies of: (1) the government’s February 18, 2025 expert disclosure cover letter (“Exhibit A”) and (2) the government’s expert witness disclosures (“Exhibits B-D”) are attached to this motion. In its letter, the government disclosed that it intends to call Special Agent Joel DeCapua of the Federal Bureau of Investigation (“FBI”), Special Agent Stephan George of the Internal Revenue Service – Criminal Investigation (“IRS-CI”), and Philip Werlau as expert witnesses; and John Pisa-Relli, Senior Law Enforcement Coordinator, Office of Foreign Assets Control (“OFAC”), U.S. Department of the Treasury, as a lay witness. (*See* Exhibit A.)

<sup>3</sup> The government’s proposed lay and expert testimony is the subject of a separate, concurrently filed, motion *in limine*.

<sup>4</sup> FBI, *FBI Statement on Attribution of Malicious Cyber Activity Posed by the Democratic People’s Republic of Korea*, Apr. 14, 2022, available at <https://www.fbi.gov/news/press-releases/fbi-statement-on-attribution-of-malicious-cyber-activity-posed-by-the-democratic-peoples-republic-of-korea>.

The government’s proposed expert witness, Joel DeCapua, Special Agent with the FBI, whom the government intends to “call[] to testify regarding the analysis and tracing of cryptocurrency transactions using blockchain data, including the tracing of criminal proceeds[,]” makes no mention of the identity of any alleged perpetrator of computer intrusion, and does not mention the Lazarus Group, or even North Korea, at all.<sup>5</sup> (*See generally* Ex. B.) Nor could he—Agent DeCapua does not purport to have any expertise on North Korea, the “Lazarus Group,” or any alleged hacking activity by such group. (*Id.*)

The April 14, 2022 FBI press release is also inherently unreliable. Legal scholars have noted that the government’s public attribution of crimes to certain state-sponsored actors without evidence can lead to abuses:

Such “trust us” attributions are problematic for any number of reasons. They may be false. They will be difficult to corroborate (or debunk) because of the lack of supporting evidence. They may foster greater consolidation of blocs with respect to internet governance and cybersecurity issues because “trust us” will only work with allies.

Kristen Eichensehr, *The Law and Politics of Cyberattack Attribution*, 67 UCLA L. REV. 520, 567, 574 (2020). Further, such “attributions-by-alert” often use “estimative language” from the intelligence community, deploying standards that are neither legally defined nor reviewable in court. *Id.* at 574.

---

<sup>5</sup> Not only does Agent DeCapua make no mention of North Korea or the “Lazarus Group” in his “expert” disclosure—he too relies on hearsay evidence as the basis of his opinion regarding alleged “criminal exploits” that were supposedly later deposited into the Tornado Cash smart contracts. (*See* Exhibit B.) This topic is more fully dealt with in the defense’s concurrently filed motions *in limine* regarding the government’s proposed lay and expert witness testimony.

Relatedly, the government has often relied on Chainalysis for attribution of hacks to North Korea—and OFAC did so in this very case<sup>6</sup>—but Chainalysis’ methodology is vague, subject to confirmation bias, and indeed totally circular, as one of its criterion for attributing a hack to North Korea is whether Tornado Cash was used to move proceeds.<sup>7</sup> Indeed, recognizing its attribution claims’ weakness, Chainalysis itself recently retracted earlier statements it had made about North Korean hacking, reducing its estimate of hacked proceeds processed through Tornado Cash in 2023 by more than \$300 million.<sup>8</sup> Given its uncertain methodology, and its admitted errors, there is no reason that Chainalysis should be credited at all—which is likely why the prosecution team has not proposed any expert evidence relying on it. Yet, Chainalysis’ acknowledged errors underscores the inherent subjectivity and lack of real data underlying the alleged attribution of hacks to North Korea.

Finally, neither the government’s purported hacking expert nor its proposed OFAC witness intends to (or is qualified to) opine that any hacks are attributable to the Lazarus Group. The government has noticed the testimony of OFAC official John Pisa-Relli, a lay witness, who apparently will only testify that the wallet address 0x098B716 charged in Count Three was a “blocked address.”<sup>9</sup> (See Exhibit A at 2-3.) The government does not intend to introduce Pisa-

---

<sup>6</sup> The discovery materials in this case evidence that OFAC repeatedly relied on Chainalysis as its source to attribute various hacks to North Korean Hackers. See e.g., USAO\_0000120-122; USAO\_0000156.

<sup>7</sup> See Erin Plante, CHAINALYSIS, *\$30 Million Seized: How the Cryptocurrency Community Is Making It Difficult for North Korean Hackers To Profit*, Sept. 8, 2022, available at <https://www.chainalysis.com/blog/axie-infinity-ronin-bridge-dprk-hack-seizure/>.

<sup>8</sup> See Chainalysis Team, CHAINALYSIS, *Report: \$2.2 Billion Stolen from Crypto Platforms in 2024, but Hacked Volumes Stagnate Toward Year-End as DPRK Slows Activity Post-July*, Dec. 19, 2024, available at <https://www.chainalysis.com/blog/crypto-hacking-stolen-funds-2025/>.

<sup>9</sup> This statement is inaccurate. The 0x098B716 address was a Specially Designated National, a sanctioned entity. But property and interests of an SDN are not “blocked” until they come into connect with a U.S. person or entity. 31 CFR 510.201(a)(3) (“All property and interests in property that are in the United States, that come within the United States, or that are or come

Relli as an expert, which is telling given that he too holds no expertise in North Korean hacking activity, which the government presumably recognized in narrowly circumscribing his proffered testimony. (*Id.*)

Simply put, the government has no evidence that any hack was in fact conducted by the Lazarus Group, so it should not be permitted to make such a claim.

## **2. In Any Event, the Identity of the Lazarus Group Is Not Relevant**

Even assuming the government could establish a connection between the Lazarus Group and the Ronin hack, evidence regarding the identity of the Lazarus Group is irrelevant to the charges in this case. To convict Mr. Storm of Count One (conspiracy to commit money laundering), the government must prove beyond a reasonable doubt that Mr. Storm conspired to do the following:

- (1) knowing that the property involved in a financial transaction represented the proceeds of some form of unlawful activity,
- (2) conduct[] or attempt[] to conduct a financial transaction
- (3) which in fact involved the proceeds of that unlawful activity,
- (4) . . . with the knowledge that the transaction was designed at least in part to conceal or disguise the nature, location, source, ownership, or control of the proceeds of the unlawful activity.

*United States v. Gotti*, 459 F.3d 296, 334 (2d Cir. 2006).

Applied to any of the above elements, the identity of the Lazarus Group is not relevant to the government's allegations that Mr. Storm conspired to commit money laundering. The government's theory is not that Mr. Storm was involved in the underlying hacking (he was not, and there is no allegation that he was), nor that he conspired with the Lazarus Group to launder money (he did not, and there is no allegation that he did). (*See, e.g.*, Dkt. 53 at 40 (government

---

within the possession or control of any U.S. person of the following persons are blocked and may not be transferred, paid, exported, withdrawn, or otherwise dealt.”). In other words, only after the property becomes subject to U.S. jurisdiction does the obligation to block, or freeze, the property kick in. E.O. 13722 § 2(a) and 31 CFR §§510.210(a)(3).

admits it does not “allege that [Mr. Storm] conspired with the hackers that laundered the proceeds of their crimes through the Tornado Cash service.”) Rather, its theory is simply that Mr. Storm knew that certain transactions using Tornado Cash’s protocol represented illegal hacking proceeds yet did nothing to stop those transactions (even though he was powerless to do so when they occurred). (*See, e.g., id.* at 13-14 (“[Mr. Storm] was fully aware that the service was processing large volumes of criminal proceeds and continued to operate the service[.]”).) Under the government’s theory, it does not matter who the hackers were; it only matters that Mr. Storm knew about the hacking, knew that the hackers were using the Tornado Cash protocol to conceal the proceeds of the illegal hacking, and willfully conspired to launder those proceeds. In sum, the Lazarus Group’s purported connection to North Korea has no relevance to whether Mr. Storm conspired to commit money laundering.

The identity of the Lazarus Group is likewise not relevant to Count Two (conspiracy to operate an unlicensed money transmitting business in violation of 18 U.S.C. § 1960(b)(1)(C)) for the same reasons. The relevant elements that the government is required to prove are that Mr. Storm conspired to “a) transfer, on behalf of the public, b) funds, and c) . . . with knowledge that the funds were derived from a criminal offense.” *See, e.g., United States v. Murgio*, 209 F. Supp. 3d 698, 706 (S.D.N.Y. 2016) (citing 18 U.S.C. § 1960) (internal quotations omitted). Again, for this offense, the identity of any alleged hackers does not matter; the only knowledge at issue is whether the funds were derived from a criminal offense. The Lazarus Group’s connection to the North Korean government, therefore, again has no relevance.

The identity of the Lazarus Group is also not relevant to Count Three (conspiracy to violate IEEPA). To prove an IEEPA violation, the government must prove that Mr. Storm knowingly and willfully entered into a conspiracy with the objective of causing a U.S. person to

deal in property of a sanctioned entity without OFAC approval. The sanctioned entity charged is the 0x098B716 Address, and the fact that the address might be affiliated with the Lazarus Group is irrelevant to IEEPA's elements. The government effectively concedes this fact, given that it offers no evidence to prove the identity of the person or entity who controlled the wallet. For the reasons set forth above, the defense is skeptical that the government could even prove that the wallet was associated with North Korea, much less specifically attribute it to the Lazarus Group. The defense is willing, however, to stipulate that the wallet address was designated as an SDN. Therefore, the government can simply use the term "sanctioned entity" without further explication. *See* Defense Proposed Jury Instructions, XVI(B).

### **3. Any Possible Probative Value of the Identity of the Lazarus Group Is Far Outweighed by Its Prejudicial Effect**

Even if the Lazarus Group had a demonstrated connection to any hacks at issue, and even if that fact was relevant to the charged offenses, its probative value would be far outweighed by its prejudicial effect and should be precluded under Federal Rule of Evidence 403. Where prejudicial evidence regarding other bad conduct is not needed to prove the elements of the charged offense, it should be excluded under Rule 403. *See Old Chief*, 519 U.S. at 180-86 (finding it unfairly prejudicial to introduce evidence of name and nature of defendant's prior conviction in felon-in-possession case where defendant offered to stipulate to fact of prior conviction). Here, the other bad conduct at issue is not even that of Mr. Storm but of an unrelated entity altogether.

The Lazarus Group refers to a group of cybercriminals sponsored by the North Korean government. Jurors can be expected to know that North Korea poses specific threats to the interests of the United States and to have strong feelings about such a threat. Any references to



the Lazarus Group, without any connection between Mr. Storm and the group, risks inflaming the jury and thus would be unfairly prejudicial.

Indeed, introducing evidence regarding the Lazarus Group is akin to introducing evidence regarding a terrorist group. “There can be little doubt that . . . evidence linking a defendant to terrorism in a trial in which he is not charged with terrorism is likely to cause undue prejudice.” *United States v. Elfgeeh*, 515 F.3d 100, 127 (2d Cir. 2008). In *United States v. Al-Moqayad*, the Second Circuit reversed the district court for allowing testimony regarding terrorist conduct that the defendant was not charged with, although the defendant was charged with providing material support to the same terrorist group. *See* 545 F.3d 139, 159-62 (2d Cir. 2008) (evidence of uncharged conduct, an eyewitness description of a terrorist bus bombing, not involving the defendant was found to be more inflammatory than the charged crime). The Second Circuit held that given the defense’s willingness to stipulate that the group was a terrorist organization, the testimony was too prejudicial, not probative, and had an unfair effect. *Id.* at 160-61. Similarly, references to the Lazarus Group and its alleged cybercrimes in support of the North Korean government would be highly prejudicial, not probative of any element of the government’s charges, and would have an unfair effect because Mr. Storm has not been charged with the Lazarus Group’s purported crimes and is not alleged to have any connection to the group.

Introducing evidence regarding the identity of the Lazarus Group would also confuse the issues, mislead the jury, cause undue delay, and waste time. *See* Fed. R. Evid. 403. As discussed above, the government’s basis for attributing the Ronin Bridge hack to the Lazarus Group remains unexplained, is unclear, and would be subject to scrutiny from the defense. While the government may rely on undisclosed evidence sources in making a public declaration or designating a wallet as blocked property, the government should not be permitted to rely on

undisclosed evidence sources in a criminal trial. Disclosure of the government's evidence sources could also lead to a mini-trial as to whether such attribution is appropriate. Evidence about the Lazarus Group would be complex, likely requiring expert testimony, and would consume undue amounts of time, given its minimal relevance to the charges. And litigating these issues runs a high risk of jurors improperly inferring that Mr. Storm had connections to the group. For these reasons, this Court should exclude any evidence regarding the identity of the Lazarus Group under Rule 403.

**B. MIL No. 2: This Court Should Preclude the Government from Introducing Victim Testimony or Referencing Victim Impacts Regarding the Lazarus Group's Hacking**

Relatedly, Mr. Storm moves for an order precluding testimony from any victims or references to the impact on victims of any alleged hacks based on irrelevance and unfair prejudice in violation of Federal Rules of Evidence 401, 402, and 403. The experience of the victims of any bad actors who hacked other protocols and routed proceeds through Tornado Cash has no relevance to proving the charges against Mr. Storm. Any references to such alleged victims will also cause him unfair prejudice.

**1. Victim Impacts Are Irrelevant in This Case**

The experience of any hack victim has no bearing on the charges at bar, and any testimony or references related to such experiences thus should be excluded under Federal Rules of Evidence 401 and 402. There is no evidence tying Mr. Storm to any bad actor's criminal conduct.

To prove conspiracy, the government must demonstrate beyond a reasonable doubt: “(1) the existence of the conspiracy charged, and (2) the participation of each defendant in that conspiracy.” *United States v. Araujo*, 539 F.2d 287, 289 (2d Cir. 1976). As to the second

element, the Second Circuit has said, “proof of criminal acts not involving [the defendants] would be irrelevant.” *Id.*

The government has produced discovery reflecting an interview with an individual who was allegedly scammed by the Lazarus Group, causing that person to purportedly lose substantial amounts of money. But Mr. Storm is not charged with the conduct that allegedly victimized this individual, and such testimony would have no bearing on the charges Mr. Storm faces. Proof of criminal acts not involving Mr. Storm should thus be excluded as irrelevant. *Id.*

## **2. The Prejudicial Effect of Victim Testimony or References Would Substantially Outweigh Any Probative Value**

Even if evidence pertaining to hacking victims were somehow relevant, the government should nonetheless be precluded from introducing it because any probative value would be substantially outweighed by the danger of “unfair prejudice, confusing the issues, misleading the jury, . . . [or] wasting time[.]” Fed. R. Evid. 403; *see United States v. Bermudez*, 529 F.3d 158, 161 (2d Cir.2008) (“courts have broad discretion to balance probative value against possible prejudice”).

“When evaluating the admissibility of victim impact testimony during trial, a district court should carefully consider the prejudicial potential of such testimony.” *United States v. Hendricks*, 921 F.3d 320, 329 (2d Cir. 2019). Victim statements are highly prejudicial because they appeal to juror sympathies, and courts in this District have routinely excluded evidence that unfairly appeals to such emotion. *See, e.g., United States v. Malka*, 602 F. Supp. 3d 510, 527 (S.D.N.Y. 2022). The Second Circuit has affirmed excluding evidence on that basis. *See, e.g., United States v. Paccione*, 949 F.2d 1183, 1201 (2d Cir. 1991) (affirming exclusion of evidence that defendant’s son had cerebral palsy because the evidence “could well cause the jury to be influenced by sympathies having no bearing on the merits of the case”).

Here, testimony from any alleged hacking victim would serve as nothing more than a tool to appeal to jurors' sympathies. Such references would unfairly prejudice Mr. Storm, who has not been charged with the Lazarus Group's criminal conduct. Furthermore, it would confuse the issues and mislead the jury into considering victims of crimes with which Mr. Storm is not charged. Likewise, it would cause undue delay and waste time to discuss matters that would not assist the government in proving their charges against Mr. Storm.

**C. MIL No. 3: This Court Should Preclude the Government from Offering Evidence or Argument Related to North Korea's Military, Including Its Weapons and Nuclear Missile Programs**

While the government has not provided any indication that it intends to offer evidence or make arguments related to North Korea's military, including weapons and nuclear missile programs, such evidence would be extremely prejudicial, and the government should be precluded from offering any such evidence or arguments pursuant to Federal Rules of Evidence 401, 402, and 403.

There is no evidence that Mr. Storm was involved in any attempt to assist the North Korean military or, indeed, had any contact with North Korea whatsoever. Thus, any implication (whether through evidence or argument) that Mr. Storm somehow assisted North Korea's military is irrelevant to the claims here, which deal solely with Mr. Storm's involvement with a decentralized cryptocurrency privacy tool, *i.e.*, the Tornado Cash protocol. Given the highly controversial nature of North Korea's military, including its weapons and nuclear missile programs, the mere mention of these topics at Mr. Storm's trial would be inflammatory, highly prejudicial, and misleading. This is precisely what Rule 403 seeks to avoid. *See Doe v. Lima*, 2020 WL 728813, at \*6 (S.D.N.Y., Feb. 13, 2020). Therefore, this Court should preclude any such evidence or argument.

**D. MIL No. 4: This Court Should Preclude the Government from Introducing Evidence or Argument Regarding So-Called Tornado Cash “Marketing Materials” that Allegedly Depict a Washing Machine**

Based on the government’s comments at the July 12, 2024 motions hearing, the defense expects the government to offer in evidence alleged marketing materials of Peppersec (an entity of which Mr. Storm was a developer) depicting a washing machine to attempt to show Mr. Storm’s criminal intent. This Court should exclude this evidence under Federal Rules of Evidence 401, 402, and 403.

The government’s relevance claim, as explained at the hearing, is expected to be that the Peppersec developers:

did in fact market the service specifically to money launderers. And there will be evidence of that at trial, and we think that will be one of the bases on which the jury can find the requisite intent to be conspiracy to commit money laundering. Just to take an example of that, the defendant created marketing materials that showed dirty ETH, and then it showed a washing machine, and the washing machine had the Tornado Cash logo on it. So it was very explicit what they contemplate their customer base wanted.

(Dkt. 69, July 12, 2024, Oral Arg. Tr. At 94:4-13.) This argument rings hollow, as it is devoid of any context concerning when and why the alleged “marketing materials” were created, and where and when they were used.<sup>10</sup> Viewed in context, the government cannot connect any dots to prove that those materials showed any intent or motive regarding Tornado Cash’s target market, and they therefore should be excluded.

As an initial matter, the fact that marketing materials were created proves nothing, and certainly does not show that Peppersec’s developers, including Mr. Storm, targeted a nefarious “customer base.” The defense understands that the “marketing materials” are nothing more than

---

<sup>10</sup> At present, the defense is not precisely sure what the purported marketing materials are, because the government will not be disclosing its exhibit list until June 30, 2025.

a crude cartoon attempting to simplify and poke fun at its subject matter, and on their face not meant to be taken literally.

Further, the alleged marketing materials were not in fact used to market to money launders. The defense believes the government will be able to show, at most, that they were used at an early and reputable Ethereum conference, ETH Boston 2019. Such ETH conferences were and are today reputable forums for academic, developer, and industry collaboration and advocacy. Indeed, ETH Boston 2018 took place at Harvard University and was marketed as bringing together “[t]he leading minds in the cryptocurrency space” from around the world to collaborate together on decentralized applications using Ethereum.”<sup>11</sup> North Korean cybercriminals would not be in attendance at ETH Boston, nor could there be any evidence of them attending. The appearance of the Peppersec developers at such conferences served exactly the opposite purpose from what the government suggests: they served to educate the Ethereum community generally about Tornado Cash, as the key to the Tornado Cash protocol’s success was widespread lawful adoption in the Ethereum community.

The so-called “marketing materials” are also irrelevant to the government’s case here because, to the defense’s knowledge, they were only used in or about fall 2019—prior to the time that any of the charged conspiracies allegedly began. The government’s alleged conspiracies began a full year later, in September 2020 (*see* Ind. ¶ 77), and there is no evidence as far as the defense is aware that Mr. Storm ever used such marketing materials after fall 2019.

Even if the alleged marketing materials were relevant to the charges, it is far more prejudicial than probative here, and thus in violation of Rule 403. Should the alleged marketing

---

<sup>11</sup> *See* CRYPTOEVENTS, *ETHBoston — September 6-8, 2019 Announcement*, available at <https://cryptoevents.global/ethboston-hackaton-2019/>.

materials be introduced in evidence, the defense will be forced to respond with evidence as to the circumstances under which they were created, the limited time period they were used, when and why Mr. Storm expressly determined they should not be used after 2019, and what type of marketing materials in fact were used, resulting in a mini-trial on tangential issues, rather than keeping the focus on the development of Tornado Cash during the time period charged in the Indictment.

For these reasons, the Court should preclude the government from introducing the purported “marketing materials.”

**E. MIL No. 5: This Court Should Preclude the Government from Introducing Any Evidence of Mr. Storm’s Alleged TORN Sales**

This Court should preclude the government from introducing any evidence of Mr. Storm’s alleged sales of TORN, which do not reflect a fee or profit from use of the Tornado Cash protocol, because it is not relevant under Rule 401 and, in any event, should be excluded under Rule 403. This Court should further exclude references to Mr. Storm’s alleged sales of TORN because it was legal to sell TORN, and presenting evidence of any alleged sales would simply confuse the jury.

For the money laundering and IEEPA conspiracy charges in the Indictment, whether or not Mr. Storm made any profit from Tornado Cash is irrelevant and prejudicial. Money laundering requires only evidence that the “financial transaction” at issue involved the proceeds of specified unlawful activity, and there is no allegation that TORN, or sales thereof, represented criminal proceeds. *See* 18 U.S.C. § 1956(a)(1).

The only issue in this case for which it would be relevant to offer evidence of a fee is the Section 1960 charge because a “money transmitting business” has been held to be a business that transmits or transfers funds for a fee. *See United States v. Velastegui*, 199 F.3d 590, 592 (2d Cir.

1999). But Tornado Cash does not charge a protocol fee or any other fee for use and is instead completely free for users. *See Van Loon v. Dep't of the Treasury*, 122 F. 4th 549, 558 (5th Cir. 2024) (noting that the only fees are gas fees to the Ethereum blockchain and optional relayer fees); *see also* Reply Brief of Plaintiff-Appellants, *Van Loon v. Dep't of Treasury*, No. 23-50669 (5th Cir. Apr. 15, 2024), 2024 WL 1771719, at \*23 (Reply Brief of Plaintiff-Appellants) (“The immutable smart contracts do not confer any fees directly to the Tornado Cash ‘entity.’... [M]any people use the immutable smart contracts without involving any relayer, and such transactions do not result in any commissions.”). The only fees paid to use Tornado Cash were the required gas fees paid directly to the Ethereum blockchain.<sup>12</sup> *See* Electronic Frontier Foundation (EFF) Amicus Brief Dkt. 122-1 at 9 (payment of gas fees is nothing more than “built-in cost required to make a transaction on the [Ethereum] blockchain” and relayers’ payment of gas fees “is nothing more than the decentralized cryptocurrency program working as it was intended”). Indeed, as noted in *Van Loon*, “Tornado Cash doesn’t profit from the immutable smart contracts” or mutable contracts. 122 F. 4th at 567. While “[s]ome relayers and TORN token holders may receive fees from using the *mutable* relayer-registry smart contracts, [they do] not [profit] from the immutable smart contracts” because the protocol does not charge any fees. *Id.* Given that there were no fees charged, the developers received no compensation from any Tornado Cash smart contract activity.

Similarly, neither the User Interface (“UI”) nor Command Line Interface (“CLI”) charged a fee, as the government admits. Simply put, the Tornado Cash smart contracts, and the free

---

<sup>12</sup> *See* COINBASE, *What Are Gas Fees?*, available at <https://www.coinbase.com/learn/crypto-basics/what-are-gas-fees> (noting that “[g]as fees... are transaction costs that users pay to execute operations on the network” and that the fees are “a form of remuneration for validators who maintain and secure the Ethereum blockchain,” thus Ethereum “[v]alidators... receive these fees”).



ancillary software tools that the developers allegedly created to assist users in accessing them, were entirely free and charged no fee. *See e.g.*, Coin Center Amicus Brief, Dkt. 43 at 12 (“[N]o fees are ever paid to the developers of the Tornado Cash protocol.”)

Recognizing that there was no fee charged by Tornado Cash, the government intends to introduce evidence of gains that the developers realized from selling their allocations of TORN as evidence of a fee for the use of the Tornado Cash protocol. But evidence of the developers’ TORN sales has no relevance to the issue of whether the alleged money transmitting business charged a fee, and should be excluded.

As an initial matter, the government has no evidence that any monies the developers earned from selling TORN were associated with the usage of the Tornado Cash protocol. When launched, and for most of the period it existed, TORN had no use case at all, and was solely a tool to increase decentralization. As the *Van Loon* court explained: “After the pool contracts became immutable, the original developers of Tornado Cash announced the creation of a decentralized autonomous organization (DAO) and a new crypto token called TORN,” which allows “individuals to vote on a limited subset of DAO governance issues.” 122 F. 4th at 557-58. When announcing the possibility of the TORN token, a Medium article by the developers stated that “TORN is an ERC20-compatible token with a fixed supply that governs Tornado.Cash” and allows TORN holders to “make proposals and vote to change the protocol via governance.”<sup>13</sup> At the time of the launch of TORN in December 2020, the Medium article made clear that “TORN is not a fundraising device or investment opportunity” and further noted that TORN would initially be non-transferable.

---

<sup>13</sup> Tornado Cash, MEDIUM, *Tornado.Cash Governance Proposal*, Dec. 17, 2020, available at <https://tornado-cash.medium.com/tornado-cash-governance-proposal-a55c5c7d0703>.

Even once the relay register was implemented in April 2022—which occurred very close to the end of the developers’ involvement with the project—it did not provide TORN holders with profit from users’ use of Tornado Cash. As explained in the Blockchain Association’s Amicus Curiae Brief, “[r]elayers are third parties who provide an additional layer of anonymity for Tornado Cash Users.” (Dkt. 45 at 12.) Relayers “process withdrawal requests on behalf of users, including paying the gas fee” and “[i]n return, relayers recoup the gas fee plus a service fee.” (*Id.*) As Coin Center explained in its Amicus Brief, while the government previously hypothesized that the requirement for relayers to hold TORN could have enriched the Tornado Cash developers, “[t]his is an extremely attenuated claim with no evidence offered” and does not create any “direct pecuniary link between any alleged users of the protocol (*e.g.* the Lazarus Group) and the Defendant[.]” (Dkt. 43 at 10.) Indeed, and to the contrary, the value of TORN plummeted during the post-relayer registry period. (*Id.* at 11.) Given that the developers’ alleged TORN sales occurred during this period, the developers only lost money after the relay network was implemented, which is the opposite of profiting from any connection that the relay network could have provided between TORN and the use of the protocol.

Moreover, even if TORN profit was linked in any way to the use of the Tornado Cash protocol (which it is not), it is not a fee for service. The definition of a fee is “an amount of money paid for a particular piece of work or for a particular right or service.”<sup>14</sup> Fees charged by a money transmitting business are fees for specific transactions or services. For example, Bank of America charges its users a \$10 fee for overdrafts, a \$30 fee for domestic wire transfers, and

---

<sup>14</sup> Fee, CAMBRIDGE DICTIONARY, available at <https://dictionary.cambridge.org/us/dictionary/english/fee>.

so forth.<sup>15</sup> Western Union advertises “four types of money transfer fees,” including (1) outgoing transfer fees (2) incoming transfer fees, (3) intermediary transfer fees; and (4) exchange fees.<sup>16</sup> Again, each of these fees is for a particular transfer service.

Further, the developers’ gains from TORN sales were not profit, much less illicit profits. Profit represents “money that is earned in trade or business after paying the costs of producing and selling goods and services.”<sup>17</sup> The government alleges that the “Tornado Cash service” was a for-profit money transmitting business. But in fact, because the smart contracts and interface charged no fees, the alleged business had no revenues, and thus no profits at all. The fact that the developers were granted allocations of TORN, which rose and fell based on various market factors, and sold some portion of their TORN for gains, does not mean that the “Tornado Cash service” earned a profit. It therefore is not relevant to any issue in dispute and should be excluded.

Evidence of Mr. Storm’s TORN sales should further be excluded as more prejudicial than probative, under Fed. R. Evid. 403. Any discussion of a defendant’s assets or wealth can be prejudicial, and an allegation that Mr. Storm made significant gains in selling TORN may confuse the jury into believing that Tornado Cash was in fact profitable when it was not. The government has also suggested that there was some impropriety in selling TORN, coupling the

---

<sup>15</sup> BANK OF AMERICA, “Personal Schedule of Fees”, May 16, 2025, available at <https://www.bankofamerica.com/salesservices/deposits/resources/personal-schedule-fees/> (overdraft fee \$10, domestic wire transfer fee of \$30).

<sup>16</sup> Western Union clarifies that, in fact, “an exchange rate isn’t necessarily a fee,” but wants users to understand it is a money transfer cost worthy of consideration. *See* Christy Lowery, WESTERN UNION, *How much are money transfer fees?*, Nov. 29, 2024, available at <https://www.westernunion.com/blog/en/us/how-much-are-money-transfer-fees/>. It also mentions that other fees may apply, such as cancellation fees, correspondent bank fees, etc. *Id.*

<sup>17</sup> Profit, CAMBRIDGE DICTIONARY, available at <https://dictionary.cambridge.org/dictionary/english/profit>.

events concerning the TORN sales with the chronology of OFAC's *ultra vires* sanctions on the Tornado Cash smart contracts. (*See ind.* ¶75 (“After the sanctions on the Tornado Cash service were announced, . . . [Mr. Storm] again accessed the Binance account” and “transferred approximately \$7.6 million worth of U.S.-dollar pegged stablecoins.”).) In fact, TORN was not sanctioned when Mr. Storm is alleged to have sold it in August 2022 and, in any event, the sanctions were found illegal and have been lifted. (*See infra* at F (MIL No. 6)). Accordingly, while it was neither nefarious nor improper for Mr. Storm to sell TORN at that time, the government's mention of the timing of the sales and the sanctions may confuse the jury and result in unfair prejudice. Given that the TORN sales do not bear on any issue in the case, the defense respectfully submits that the balance tilts toward excluding this evidence under Fed. R. Evid. 403.

**F. MIL No. 6: This Court Should Preclude the Government from Characterizing Mr. Storm's Alleged Sales of TORN Using Language that Reflects a Legal Conclusion or Is Inflammatory, Confusing, or Unduly Prejudicial, Including by Referencing His Russian Background**

In the alternative, should this Court permit the government to reference Mr. Storm's TORN sales, pursuant to Federal Rules of Evidence 401, 402, and 403, this Court should preclude the government and its witnesses from characterizing Mr. Storm's alleged 2022 TORN sales using language that is inflammatory, confusing, or unduly prejudicial. Crucially, it was not illegal to sell TORN then, and it is not illegal to sell TORN now. While there was an interim period where OFAC sanctioned TORN, as discussed further below, the Tornado Cash sanctions were later ruled illegal in *Van Loon*, 122 F.4th 549 (5th Cir. 2024), and lifted on March 21, 2025.

Evidence of Mr. Storm's alleged sales of TORN is, at most, relevant to just one of the three charges: Count Two, the alleged conspiracy to operate an unlicensed money transmitting business in violation of 18 U.S.C. § 1960. To prove such a violation, the government must prove

that the alleged money transmitting business is “(1) an enterprise (not a single transaction) (2) that is conducted for a fee or profit.” *United States v. Banki*, 685 F.3d 99, 113 (2d Cir. 2012). But even assuming Mr. Storm’s alleged sales of TORN are probative of the “profit” element of Count Two and thus admissible, “courts often prohibit the use of certain ‘pejorative terms when such categorizations [are] inflammatory and unnecessary to prove a claim’ and such statements ‘do not bear on the issues being tried.’” *MF Global Holdings, Ltd. V. Pricewaterhouse Coopers LLP*, 232 F. Supp. 3d 558, 570 (S.D.N.Y. 2017) (quoting *Aristocrat Leisure Ltd. V. Deutsche Bank Trust Co. Americas.*, 2009 WL 3111766, at \*7 (S.D.N.Y. Sept. 28, 2009)); *see also United States v. Smothers*, 652 F. Supp. 3d 271, 284 (E.D.N.Y. 2023) (“Although evidence may be relevant as directly probative of, or inextricably intertwined with, the defendant’s charged conduct, this evidence may nonetheless be inadmissible pursuant to [Rule 403] if its probative value is substantially outweighed by a danger of unfair prejudice.”) (citation omitted). Here, the government has made several inflammatory allegations that it should be precluded from raising at trial.

First, the government has made thinly veiled references to Mr. Storm’s Russian background, which, if presented to a jury, would be highly prejudicial and irrelevant due to the widespread negative image of Russia in the United States. The Indictment alleges that Mr. Storm, “[i]n an effort to conceal” the Peppersec developers’ TORN sales, sold a portion of their TORN tokens “through an account held in the name of another person, a Russian national, at Binance, a cryptocurrency exchange.” (Ind. ¶ 73.) The Indictment also cites an alleged statement by Mr. Storm that he “did everything from Russian Binance...and even from a Russian IP (VPN).” (*Id.*) Such allegations are highly prejudicial and irrelevant, as the manner in which Mr. Storm sold TORN has no bearing on the question of whether such sales reflect the profits of

an alleged money transmitting business. The government’s subtle references to Mr. Storm’s connections to Russia, at a time when Russia’s favorability view among Americans is at a mere 9%,<sup>18</sup> can serve no purpose other than to stoke the jury’s emotions against him. Because such references are “inflammatory and unnecessary to prove a claim” and “do not bear on the issues being tried,” *MF Global*, 232 F. Supp. 3d at 570, this Court should preclude the government from making any reference to Mr. Storm’s alleged use of a “Russian national’s” account or a VPN to access a “Russian Binance account” in connection with his alleged sales of TORN.

Second, this Court should preclude the government from presenting any evidence purporting to show *why* Mr. Storm allegedly sold TORN in the manner that he purportedly did, as such allegations are, once again, not probative of any elements of the charges he faces. The government alleges that Mr. Storm sold TORN through the Binance account “for the purpose of selling them without revealing those sales to the public, including other holders of TORN tokens.” (Ind. ¶ 73.) Whether or not that is true—and to be clear, it is not—Mr. Storm’s motivations for effectuating the alleged sales in a particular manner have no bearing on whether such sales reflect the profits of an alleged money transmitting business. Nor do Mr. Storm’s motivations have any bearing on the other conspiracy charges he faces. As such, these allegations are “more inflammatory than the charged crime,” *Livoti*, 196 F.3d at 326, and risk “lur[ing] the factfinder into declaring guilt on a ground different from proof specific to the offense charged.” *Old Chief*, 519 U.S. at 180. Requiring Mr. Storm to present a defense against this allegation would “open up a flood of evidence regarding a possibly confusing collateral issue.” *United States v. Gleason*, 616 F.2d 2, 23 (2d Cir. 1979). As such, this Court should

---

<sup>18</sup> See Jeffrey M. Jones, GALLUP, *Americans’ Favorable Rating of Russia Sinks to New Low of 9%*, (Mar. 13, 2023) available at <https://news.gallup.com/poll/471872/americans-favorable-rating-russia-sinks-new-low.aspx>.

preclude the government from presenting any evidence regarding the manner of, or the motivations for, Mr. Storm's purported sales of TORN, which are not relevant.

Finally, this Court should preclude evidence of Mr. Storm's alleged statements to the Peppersec developers after the sale of TORN for similar reasons. The government alleges that Mr. Storm "sent further messages advising [the Peppersec developers], in substance, to conduct further transactions to make it more difficult to trace these funds, saying, 'my personal advice: create new wallets, new seed phrases, transfer money to new addresses.'" (Ind. ¶ 75.) Again, Mr. Storm's statements to the Peppersec developers about what they should or should not do with the TORN in their wallets is irrelevant to any elements of the charges Mr. Storm faces. As an initial matter, there were perfectly lawful and valid reasons for Mr. Storm to offer that advice. But more to the point, concealing or "mak[ing] it more difficult to trace" the alleged profits from what the government argues is a money transmitting business, even if proven, is simply not an element of any of the charges Mr. Storm faces. The government seeks to introduce these statements not for their probative value but to prejudice the jury against Mr. Storm, and this Court should therefore preclude the government from presenting post-sale statements by Mr. Storm that are not probative of any of the elements of the offenses charged.

**G. MIL No. 7: This Court Should Preclude the Government from Introducing Evidence or Argument Referencing OFAC's Imposition of Sanctions on Tornado Cash Without Mentioning That The Sanctions Were Held to Be Unlawful**

Should this Court allow the government to introduce evidence about TORN over the defense's above objections, then the defense requests an order that the government and its witnesses be precluded under Rules 401, 402, and 403 from introducing evidence or making references to OFAC's imposition of sanctions on Tornado Cash without also mentioning that courts later found the sanctions unlawful because OFAC lacked authority to impose them.

Reference to any sanctions on Tornado Cash without the context that the sanctions were ultimately struck down by courts would be unfairly prejudicial and mislead the jury.

On November 26, 2024, the Fifth Circuit decided *Van Loon*, , holding that the sanctions entered against Tornado Cash “property” were unlawful because the immutable smart contracts at issue cannot be considered “property” under the IEEPA.<sup>19</sup> On March 21, 2025, the Treasury Department announced that it would “remove the economic sanctions against Tornado Cash” in light of “the novel legal and policy issues raised by use of financial sanctions against financial and commercial activity occurring within evolving technology and legal environments.”<sup>20</sup> That same day, the Treasury Department filed a notice in the district court that “Tornado Cash is no longer subject to sanctions by [OFAC], and this matter is now moot.” *See Van Loon v. Dept of the Treasury*, No. 1:23-cv-312-RP, ECF No. 107 (W.D. Tex., Mar. 21, 2025). Both the press release and filing included a link to the updated list of specially designated nationals, which shows that *all* sanctions imposed on Tornado Cash property—not just those directed at the immutable smart contracts—had been removed.<sup>21</sup>

In another case challenging the Tornado Cash sanctions in the Eleventh Circuit, the Treasury Department filed multiple motions to hold the appeal in abeyance in light of the delisting and ongoing discussions with the plaintiffs regarding next steps.<sup>22</sup> On April 28, 2025, the district court entered an order granting the plaintiff’s motion for entry of judgment and, after

---

<sup>19</sup> OFAC defined Tornado Cash “property” as including “open-source computer code known as ‘smart contracts.’” *Van Loon*, 122 F.4th at 553.

<sup>20</sup> Press Release, DEP’T OF TREASURY, *Tornado Cash Delisting*, Mar. 21, 2025 available at <https://home.treasury.gov/news/press-releases/sb0057>.

<sup>21</sup> *See* OFAC, *Cyber-related Designation Removal; North Korea Designation Update and Removal*, Specially Designated Nationals List Update, Mar. 21, 2025, available at <https://ofac.treasury.gov/recent-actions/20250321>.

<sup>22</sup> *See Coin Center, et al. v. Secretary, Dep’t of Treasury, et al.*, Case No. 23-13698, ECF Nos. 54, 56, 58 (11th Cir. Apr. 21, 2025).



vacating its prior order granting the government’s motion for summary judgment, entered an amended final judgment finding that the government’s “action is unlawful and is therefore set aside” and that the government is “permanently enjoined from enforcing it.” *Van Loon*, No. 1:23-cv-312-RP, ECF No. 111 at 1.

As discussed above, the indictment suggests that the government intends to offer evidence that Mr. Storm sold TORN after the time of the sanctions to suggest that such sales were improper. Specifically, the government alleges that after the announcement of the Tornado Cash sanctions, Mr. Storm “accessed the Binance account, where he was holding at least approximately \$8 million worth of cryptocurrency that represented the proceeds of sales of TORN tokens[,]” and later transferred \$7.8 million worth of U.S.-dollar pegged stablecoins from the Binance account.” (Ind. ¶ 75). This evidence should be precluded.

As an initial matter, there was nothing unlawful about Mr. Storm selling TORN in August 2022. TORN was not sanctioned at that time, and the imposed sanctions were later found illegal. The *Van Loon* decision in fact fully supports that Mr. Storm could not have knowingly and willfully conspired to commit money laundering and IEEPA sanctions violations because he lacked any ability to control what any user did with the immutable smart contracts.

Indeed, in finding that the smart contracts at issue were not property capable of being owned, much less sanctioned, the Fifth Circuit observed that “no one can ‘exclude’ anyone from using the Tornado Cash pool smart contracts.” *Van Loon*, 122 F.4th at 565. And in rejecting the Department’s argument that the Tornado Cash smart contracts at issue were a “code-enabled species of unilateral contracts,” the Fifth Circuit found that “[e]ven assuming the Tornado Cash developers made an offer by creating the smart contracts and publicizing the code to be used for mixing and pooling, they revoked their offer—and any role in it—by changing the code to be

immutable, thus running independently and autonomously.” *Id.* at 568-69. The Fifth Circuit further observed:

Tornado Cash has no control over these immutable smart contracts. It cannot change the code, delete the code, or remove the code from the Ethereum blockchain network. In other words, Tornado Cash cannot “unplug” the immutable smart contracts. Even if Tornado Cash did not want North Korea, the Lazarus Group, or anyone else, for that matter, using the immutable smart contracts that the Tornado Cash developers created, Tornado Cash—let alone the Department—would be powerless to stop them.

*Id.* at 569.

Here, if reference were made at trial to the Tornado Cash sanctions without the information that they were subsequently determined by a court to be unlawful, it could improperly suggest to the jury that they should reach the same (erroneous) conclusion as OFAC when it first imposed the sanctions—that Tornado Cash knowingly dealt with sanctioned property, specifically that of the Lazarus Group. *See, e.g., United States v. Klein*, 2017 WL 1316999, at \*8 (E.D.N.Y. Feb. 10, 2017) (declining to allow the introduction of an SEC complaint under Rule 403 because it would be suggestive to the jury that they should reach the same conclusion the agency did as to the charged conduct). Such a conclusion would be at odds with the view of the Fifth Circuit in *Van Loon*, which overruled OFAC.

For all these reasons, this Court should exclude evidence of or references to the illegal Tornado Cash sanctions pursuant to Federal Rules of Evidence 401, 402, and 403.

**H. MIL No. 8: This Court Should Preclude the Government From Arguing That Anonymous Blockchain Activity or Crypto-Mixing Is Illicit**

The defense moves to preclude any government statements suggesting that crypto-mixing protocols, or anonymizing software protocols more generally, are inherently suspicious or constitute illicit activity, pursuant to Federal Rules of Evidence 401, 402, and 403. Any such

suggestion would be legally inaccurate and likely to unfairly prejudice Mr. Storm and confuse the jury.

The government has acknowledged in its briefing that Tornado Cash had the legitimate goal of enhancing privacy for transactions on the blockchain. (*See e.g.*, Dkt. 53 at 31 (“nothing in this case indicates that cryptocurrency mixing services themselves are illegal”).) Elsewhere, however, the government, while careful in its phrasing, appears to suggest that anonymous blockchain transactions—and dealing in cryptocurrency in general—serve nefarious purposes. (*Id.* at 3 (noting that cryptocurrency is the “preferred asset class of many criminals but especially cybercriminals”); *id.* (alleging that Tornado Cash’s “features were of immense value to cybercriminals”); *id.* at 13 (noting that “[b]ecause the Tornado Cash service enabled untraceable cryptocurrency transfers, . . . it quickly became a haven for money laundering”).)

The government should not be permitted to make broad-brush arguments that blockchain applications providing for anonymity are indicative of criminality. The same would be true if, instead of a case involving cryptocurrency, the case involved traditional banking or medical services, industries which also rely heavily on privacy and shielding access to personally identifiable information.

Arguments suggesting that anonymity equals criminality would mislead the jury into believing that Tornado Cash cannot (and does not) serve any legitimate purpose. To the contrary, federal courts have explicitly held that “it is not per se unlawful to mix cryptocurrency.” *See, e.g., United States v. Sterlingov*, 2023 WL 2387759, at \*8 (D.D.C. Mar. 6, 2023). Even under current Department of Justice policy, mixers should not be prosecuted for the acts of their end users. (*See* Deputy Attorney General Todd Blanche’s April 7, 2025,

Memorandum, *Ending Regulation by Prosecution*, at 1.)<sup>23</sup> And as explained above and at length in the motion to dismiss briefing, there are numerous legitimate benefits to blockchain anonymizing protocols, including Tornado Cash. (*See, e.g.*, Dkt. 45 at 9-10 (“Tornado Cash solves these problems by protecting the privacy of individuals conducting digital asset transactions, the vast majority of which are legitimate.” (collecting authorities)).) Any narrative that crypto-mixing, or anonymous activity on the blockchain, is an illicit practice would distort that truth and be plainly more prejudicial than probative in this case. *Cf. United States v. Guo*, 2024 WL 2262706, at \*4 (S.D.N.Y. May 17, 2024) (precluding government from eliciting “references to cryptocurrency frauds” as “prejudicial”).

Accordingly, this Court should preclude any suggestion that engaging in anonymous blockchain transactions, or the software or protocols that enable such activity, implies illicit activity.

**I. MIL No. 9: This Court Should Preclude the Government and Its Witnesses from Referring to Tornado Cash as a “Service” and Its Users as “Customers”**

This Court should preclude the government and its witnesses from referring to Tornado Cash and its users by anything other than “Tornado Cash” and “users.” The government’s submissions in this case demonstrate that it intends to refer to Tornado Cash as the “Tornado Cash service” and to the users of Tornado Cash as “customers.” (*See, e.g.*, Ind. ¶¶ 1, 3, 10, 13-22, 24-25.) Likewise, the government’s expert witness disclosures by Special Agent Joel DeCapua of the FBI, Special Agent Stephan George of IRS-CI, and Philip Werlau demonstrate their intent to parrot the government’s terminology, using “Tornado Cash service” and “customers,” in their respective expert disclosures. (*See* Exhibit B-D, respectively.) This Court

---

<sup>23</sup> Available at <https://www.justice.gov/dag/media/1395781/dl?inline>.

should preclude the use of such terms by the government’s witnesses because, in the context of this case, those terms amount to legal conclusions, which are ultimate issues for the jury to decide. A central question for the jury to decide is whether Tornado Cash was, in fact, a “service” and whether its users were “customers” such that the required elements of the charged offenses are met.

Additionally, this Court should preclude such terminology from being used by the government and its witnesses under Fed. R. Evid. 403 because there is no factual basis for the government’s nomenclature of the “Tornado Cash service”—the term is entirely of the government’s creation. Tornado Cash, as a project, has never used the term “service.” Indeed, there is nothing in the Tornado Cash literature<sup>24</sup> that ever characterizes it as the “Tornado Cash service.” Nor is there evidence that there is a public understanding of Tornado Cash as the “Tornado Cash service.” Likewise, the use of “customer” as a term to describe Tornado Cash users is not based in fact and is instead designed to bolster the government’s allegations that Tornado Cash is a “money transmitting business.” In this way, its deployment at trial would carry the additional risk of misleading the jury.

**1. This Court Should Preclude the Government’s Witnesses From Using the Terms “Service” and “Customer” Because the Terms Imply Legal Conclusions**

The defense expects the government’s experts to use the terms “service” and “customers” as set forth in their expert disclosures. The defense likewise expects other witnesses to parrot this government-created terminology. Neither the government’s expert witnesses nor its lay witnesses should be permitted to offer testimony characterizing the Tornado Cash smart contracts and related applications as a “service,” nor should they be permitted to characterize its

---

<sup>24</sup> The Tornado Cash literature refers to the Tornado Cash Whitepaper, its Medium posts, its website, and other official written material from the project.

users as “customers.” The terms are suggestive of legal conclusions—a practice that is disallowed under the Federal Rules of Evidence. *See, e.g., In re Term Commodities Cotton Futures Litig.*, 2020 WL 5849142, at \*13 (S.D.N.Y. Sept. 30, 2020) (“[W]itnesses ‘may not present testimony in the form of legal conclusions.’”). Courts in this District have precluded the government from using such terms because they “presume the ultimate issue before the jury.” *See, e.g., United States v. Ray*, 2022 WL 558146, at \*25-26 (S.D.N.Y. Feb. 24, 2022) (precluding the government from using the term “victim” outside of opening and summation and finding persuasive cases “that it constitutes improper vouching and is inconsistent with the constitutional presumption of innocence for the Government and its witnesses to refer to complaining witnesses as ‘victims’ in a case where the defense is that no crime occurred”); *United States v. Wagner*, 2022 WL 19179, at \*6 (S.D.N.Y. Jan. 3, 2022) (granting defense motion to preclude government from using the word “victim” during trial).

In particular, the Second Circuit has cautioned that government witnesses, such as experts, should not use terms that reflect legal conclusions at trial. For example, in *United States v. Scop*, 846 F.2d 135 (2d Cir. 1988), the Circuit reversed convictions where the district court allowed a government expert witness in a securities fraud case to repeat words like “manipulation,” “scheme to defraud,” and “fraud” before the jury—*i.e.*, “statutory and regulatory language” that is not “self-defining,” is “subject of diverse judicial interpretation,” and is “indicat[ive of] guilt.” *Id.* at 140–42. The Second Circuit further held that this testimony was not helpful to the jury, but instead was “calculated to ‘invade the province of the Court to determine the applicable law and to instruct the jury as to that law.’” *Id.* at 140 (quoting *FAA v. Landy*, 705 F.2d 624, 632 (2d Cir. 1983)).

Here, the government’s witnesses’ use of “service” and “customers” is similarly prejudicial and perilous due to the government’s likely theories of guilt as to Count Two, which charges Mr. Storm with “conspiracy to operate an unlicensed money transmitting business” under 18 U.S.C. § 1960, and requires the government to prove that Mr. Storm conspired to operate a “money services business” under the statute. A “money transmitting business” is a business that, for a fee, accepts funds and transfers such funds on behalf of the public. 18 U.S.C. § 1960(b)(2); *see Velastegui*, 199 F.3d at 592. But Tornado Cash, of course, does not charge any fee, nor does the UI that the Tornado Cash developers created. The government has therefore sought to use the term “service” as an artificial means to intermingle not only the Tornado Cash smart contracts, but also ancillary tools developed to use the smart contracts, such as the UI and relayer registry.<sup>25</sup>

The government has simply invented the term “Tornado Cash service” to encompass all of these tools, and characterize Tornado Cash as an entity that engaged in “money *services*.” The terms “service” and “customer,” are conclusory and cannot be employed as a substitute for evidence. The government’s characterization would improperly mislead the jury into assuming that Tornado Cash satisfies the “business” and “for a fee” elements to qualify as a “money

---

<sup>25</sup> As the EFF explains in its Amicus Brief: “[C]reating a website, user interface or back-office software for a dual-use tool should not be a basis for liability. . . . [C]riminal liability should not rise or fall based on whether a dual-use toolmaker shipped its product with a user manual.” (Dkt. 122-1 at 4-5.) Similarly, as to the relayer network,

[w]hat the government describes as some nefarious scheme by which Mr. Storm received kickbacks based on illegal transactions is nothing more than the decentralized cryptocurrency program working as it was intended. . . . The argument is akin to claiming that Visa or MasterCard would be criminally liable based solely on receiving transaction fees whenever its customers transferred money as part of some underlying criminal activity.

(*Id.* at 5).

transmitting business” for purposes of Count Two. Allowing the government to use these terms at trial would predispose the jury’s determination on an ultimate issue, violate the presumption of innocence, and lessen the government’s constitutionally mandated burden of proof.

The disclosed expert reports make clear that the government has required its experts to adopt this terminology, as they each refer to Tornado Cash as the “Tornado Cash service,” and to its users as “customers” repeatedly. Indeed, Philip Warlau’s 12-page disclosure uses the term “Tornado Cash service” **45 times**; Stephan George’s 5-page disclosure uses the term **12 times**; and Joel DeCapua’s 4-page disclosure uses the term **6 times**. There is absolutely no foundation for the use of this term by these experts. Indeed, across the industry, decentralized protocols do not use the word “customer”—which means “a person who buys goods or services”<sup>26</sup>—as it is simply incompatible with a free and open-source decentralized protocol available to anyone with an internet connection.

These experts cite no foundation for using these terms and there is none; they are clearly just shilling for the government outside of their areas of expertise. This is inappropriate and should be precluded. As this Court has held: “It is particularly inappropriate for a witness to track the exact language of statutes and regulations which the defendant is accused of violating.” *United States v. Jacques Dessange, Inc.*, 2000 WL 294849, at \*2 (S.D.N.Y. Mar. 21, 2000) (citing *United States v. Duncan*, 42 F.3d 97, 101 (2d Cir. 1994)). The government should not be permitted, through the use of conclusory unfounded legal language, to invade the province of the jury on an ultimate issue in the case: whether Tornado Cash was a “service” or “business” or, instead, merely a collection of smart contracts and related applications that gave users the tools

---

<sup>26</sup> Customer, CAMBRIDGE DICTIONARY, available at <https://dictionary.cambridge.org/us/dictionary/english/customer>.



to maintain privacy over their otherwise public transactions on the blockchain. *See* 2

Weinstein’s Federal Evidence § 403.04[1][b] (“Unfairness may be found in any form of evidence that may cause a jury to base its decision on something other than the established propositions in the case. . . . Prejudice is also unfair if the evidence was designed to elicit a response from the jurors that is not justified by the evidence.”).

## **2. The Terms “Service” and “Customer” Are Not Probative and Are Unduly Prejudicial**

This Court should also preclude the government and its witnesses from using the terms due to their minimal probative value and the immense danger of unfair prejudice. Courts in this District routinely preclude parties from using terms when a term’s probative value is outweighed by its misleading nature. *See, e.g., Highland Cap. Mgmt., L.P. v. Schneider*, 551 F. Supp. 2d 173, 193 (S.D.N.Y. 2008) (precluding terms on the basis that the use of the terms “may lead a juror to believe that the [Defendant] engaged in improper or illegal conduct”); *see also United States v. Patel*, 2023 WL 2643815, at \*12 (D. Conn. Mar. 27, 2023) (“Where a term has a low probative value . . . courts have excluded the term’s use because its probative value was outweighed by its unfairly prejudicial effect.”).

There is no probative value in the government or its witnesses using the government’s made-up terms. On the other hand, the danger of unfair prejudice is immense—the terms “Tornado Cash service” and “customers” are designed to suggest to the jury that Tornado Cash is a “money transmitting business” without requiring the government to sustain its burden to proof. The government cannot escape its burden by clinging to its own invented and prejudicial terms. For this reason too, this Court should preclude the government and its witnesses from using the terms “Tornado Cash service” and “customers.”

**J. MIL No. 10: This Court Should Preclude the Government and Its Witnesses From Offering Improper Summary Charts or Summary Testimony**

Although the government has yet to disclose its exhibit or witness list, the defense expects, as it has become routine in this District, that it will call a law enforcement agent or paralegal unfamiliar with the facts of this case as a “summary witness,” to introduce “summary charts.” Frequently, that testimony strays far beyond the permissible scope of the evidentiary rules, becoming in essence a mid-trial closing argument.<sup>27</sup> Accordingly, the defense moves to limit any summary testimony or exhibits to their allowable scope.

Federal Rule of Evidence 1006 permits the use of “a summary chart or calculation to prove the content of voluminous writings, recordings, or photographs that cannot be conveniently examined in court.” In other words, the summary is offered as a substitute for the underlying documents because the documents themselves are too lengthy to review. *See Walker v. Time Life Films, Inc.*, 784 F.2d 44, 52 (2d Cir. 1986) (“The Rule is designed to deal with the problem of writings, recordings, or photographs which cannot conveniently be examined in court by allowing them to be presented in chart or summary form.” (internal quotation marks and alteration omitted)).

But too often, rather than meeting the purposes of Rule 1006, the charts—typically, a collection of slide decks prepared by the government—selectively summarize the government’s case-in-chief. Instead of a legitimate substitute for voluminous facts, they are used as argument. The practice is deeply prejudicial to the defendant. As a result, judges in this District and

---

<sup>27</sup> Local practitioners and commentators have observed a “growing, and disturbing, trend taking place in federal criminal practice” by which the government essentially delivers summations through the use of summary witnesses and exhibits pursuant to Rule 1006. *See* Paul Townsend, “Summary Witnesses and Due Process,” N.Y.L.J. (Dec. 12, 2022). Specifically, the exhibits offered become “more akin to written closing arguments than to the summaries of voluminous writings contemplated by Rule 1006.” James Truss, “Summaries May Help, but Must Still Meet Rules 611(a), 1006,” Am. Bar Assoc. (July 18, 2012).

elsewhere have begun to police this tactic. Just last fall, Judge Liman excluded, in a commodities fraud trial, three summary charts that the government sought to offer through an FBI agent, who otherwise was not involved in the investigation or case. *United States v. Neil Phillips*, Case No. 22-cr-138, (S.D.N.Y. Oct. 20, 2023), ECF No. 90 at 2-4, 8 (hereafter “*Phillips Tr.*”).<sup>28</sup> In granting the defense motion under both Rules 1006 and Rule 403, Judge Liman noted that the charts carried “a number of risks” that “substantially outweighed” their value, including “(1) that the charts will be used in the jury room . . . as a summary of the government's summation without the defense having the opportunity of a summary of its summation also being sent into the jury room; (2) that the jury’s time will be wasted; and (3) that the evidence is needlessly cumulative to what has already been presented.” *See id.* at 4. Judge Liman explained that just because “the Court has the power to permit the receipt of the summary charts does not mean that it should exercise that power.” *Id.* at 2-3.

Judge Liman ultimately permitted the government to use the summary charts as “demonstrative aids,” but allowed considerable cross-examination (*i.e.*, over 50 pages of transcription) into whether the summary witness conducted an “independent investigation” as to whether the demonstratives portrayed an accurate picture of the case. *See, e.g., Phillips Tr.* at 83-84 (ruling, over government’s repeated objection, that extensive cross-examination was “proper, given what was presented to the jury [by the government’s summary witness] for [the defense] . . . to establish two propositions[:] . . . that the witness did not exercise any independent judgment and that the judgment was exercised by a party that has a stake in the outcome of this case regardless of what justice may have said about the government's interest being in the right

---

<sup>28</sup> For this Court’s convenience, the transcript excerpts from Judge Liman’s rulings and the subsequent cross-examination of the summary witness are attached hereto as Exhibit E.

outcome rather than a victory. . . . Number two, I think it is fair to point out the holes [in the summary testimony and/or charts]”).

Even as mere aids, any summary charts must conform to the newly revised version of Federal Rule of Evidence 107 and not be substitutes for argument.<sup>29</sup> The revised Rule 107, which took effect on December 1, 2024, only permits the use of summary exhibits as an “illustrative aid” where they would “help the trier of fact understand the evidence or argument if the aid’s utility in assisting comprehension is not substantially outweighed by the danger of unfair prejudice, confusing the issues, misleading the jury, undue delay, or wasting time.” Fed. R. Evid. 107(a) (eff. Dec. 1, 2024). The amendment’s advisory committee notes specifically prohibit aids that are “prepared to distort or oversimplify the evidence presented, or stoke unfair prejudice.” *See id.* (advisory committee notes).

Then-District Judge Nathan addressed an attempt to misuse such an aid in *United States v. Maxwell*, in which the government sought to call as a witness an FBI agent, not as a Rule 1006 summary witness, but instead to “analy[ze]” exhibits and “connect up several exhibits and review them in a way to make those exhibits clear to the jury.” *United States v. Maxwell*, 20 CR 330 (AJN) (S.D.N.Y. Dec. 9, 2021), ECF No. 757 at 7.<sup>30</sup> The government explained that the agent’s testimony would “review [the exhibits] in a way to make those exhibits clear to the jury and publish them to show, for example, the continuity of certain phone numbers and names,

---

<sup>29</sup> The advisory committee notes to the new version of Rule 107 acknowledge that the proper use of illustrative aids was previously governed by “Rule 611(a)” but “is now to be regulated by the more particularized requirements of this Rule 107.” Fed. R. Evid. 107 (advisory committee notes).

<sup>30</sup> For this Court’s convenience, the transcript excerpts from Judge Nathan’s ruling are attached hereto as Exhibit F.

where they change over time, where they are in the message books in order to make that clear for the jury.” *Id.*

Judge Nathan readily rejected this as a backdoor attempt to make two closing arguments. As the court explained, the agent’s anticipated testimony was a “streamlined version of the closing argument.” *Id.* at 15; *see also id.* at 13 (Court: “You’re simply asking [the agent] to do the work of the government in the closing.”); *id.* at 15 (Court: “That’s what this is, it’s closing argument.”). Predictably, the agent was not involved in the investigation and had no personal knowledge of the evidence. *Id.* at 13. Thus, the court precluded the anticipated testimony.

Other courts have been equally vigilant against the misuse of illustrative aids, noting that the purpose of summary charts under either Rule 107 or Rule 1006 is not to present argument, and the prosecution must not be allowed to give a mid-trial summation through such charts. *See United States v. Fullwood*, 342 F.3d 409, 414 (5th Cir. 2003) (“summary witnesses are not to be used as a substitute for, or a supplement to, closing argument.”); *see also Peat, Inc. v. Vanguard Research, Inc.*, 378 F.3d 1154, 1159-60 (11th Cir. 2004) (“because ‘summaries are elevated under Rule 1006 to the position of evidence, care must be taken to omit argumentative matter in their preparation lest the jury believe that such matter is itself evidence of the assertion it makes.” (citation omitted)). Rather, summary charts must be “nonprejudicial” and presented in a “nonmisleading manner.” *United States v. Bray*, 139 F.3d 1104, 1110 (6th Cir. 1998) (citations omitted). While the difference between valid summary testimony and argument is not a bright line, Circuit courts have made clear that the “summary should not draw controversial inferences or pronounced judgment; these functions are best left to the closing argument of counsel.” *See United States v. Lemire*, 720 F.2d 1327, 1350 (D.C. Cir. 1983); *see also United States v. Johnson*, 54 F.3d 1150, 1162 (4th Cir. 1995) (finding the “use of summaries—be it through

narrative or charts—is best saved for the prosecutor's closing argument”). Indeed, “a summary [chart] containing elements of argumentation could very well be the functional equivalent of a mini-summation by the chart’s proponent every time the jurors look at it during their deliberations.” *Bray*, 139 F.3d at 1110.

This Court should guard against the same danger here. These charts often serve the exact purpose of a closing argument—linking together evidence admitted across several different witnesses or sources and highlighting portions that arguably support the government’s theory of the case.

The risk of unfair prejudice is heightened by the fact that the government almost always attempts to introduce these sorts of exhibits through a witness with no personal knowledge of the case and no personal knowledge of the underlying documents, leaving the defense without the ability to meaningfully cross examine the witness about the material. Moreover, such presentations are by their very nature unnecessarily cumulative, as they merely highlight evidence contained in properly admissible exhibits and testimony. *See* Fed. R. Evid 107 (permitting exclusion of illustrative aids due to “wasting time” or “undue delay”); *Phillips Tr.* at 4 (noting the proposed charts are “needlessly cumulative to what has already been presented”).

While this Court could instruct the jury that any “illustrative aid” is not evidence, *see* Fed. R. Evid. 105, any limiting instruction would be insufficient to cure the harm from the equivalent of a mid-trial closing argument. Precluding the presentation is the only way to ensure Mr. Storm is not unfairly prejudiced. The government already has two opportunities to address the jury in closing, as compared to the one for the defense; it should not be given a third.

Accordingly, Mr. Storm respectfully requests that this Court preclude the government’s use of improper summary testimony or exhibits that are used as argument rather than a true

summary of voluminous facts. To the extent the government intends to use summary exhibits as illustrative aids, the defense moves for advance disclosure of such charts to give “sufficient opportunity for analysis by [the defendant], particularly if they are complex.” Fed. R. Evid. 107 (advisory committee notes); *see also id.* (“Many courts require advance disclosure of illustrative aids, as a means of safeguarding and regulating their use.”). Lastly, if this Court does permit the government to offer any charts as aids, defense counsel should be given the opportunity to conduct a thorough cross-examination like the one permitted by Judge Liman in *Phillips*.

#### IV. CONCLUSION

For the foregoing reasons, Mr. Storm respectfully requests that this Court grant these motions *in limine*.

DATED: June 6, 2025

Respectfully submitted,

By: /s/ Brian E. Klein

Brian E. Klein  
Keri Curtis Axel  
Becky S. James  
Kevin M. Casey  
Viviana Andazola Marquez  
Waymaker LLP

-and-

David E. Patton  
Nicholas D. Pavlis  
Hecker Fink LLP

*Attorneys for Roman Storm*